Methodology and Model to Establish Cybersecurity for National Security in Africa using South Africa as a Case Study

by

Johanna Christina Jansen van Vuuren

Student Number:11640629

Submitted in fulfilment of the requirements for the degree of in the subject of

Doctor of Philosophy (PhD) in Business Management

at the University of Venda

Supervisor: Dr JJ Zaaiman

Co-supervisors: Dr L Leenen, Prof A Kadyamatimba

26 February 2016

Abstract

National governments have the responsibility to provide, regulate and maintain national security; cybersecurity is an important aspect of national security and the safekeeping of a nation's constituency and resources, which includes both cybersecurity and human security for their citizens. Although all countries are vulnerable to cybercrime, African countries are particularly vulnerable to cybercrimes due to the exponential growth in broadband access, the use of wireless technologies and infrastructure, high levels of computer illiteracy and ineffectual or insufficient legislation to deal with cyberattacks and threats (Jansen van Vuuren, Phahlamohlaka et al., 2010a). South Africa was already rated as the third highest country for cyberattacks (cybercrime and other attacks) (Amit, 2011) and in 2015 as the highest in the world for phishing attacks (Symantec, 2015).

The aim of this research is to model cybersecurity policy implementation in Africa using South Africa as a case study. This proposed cybersecurity policy implementation framework will support the process of the implementation of cybersecurity in African countries to effectively control and protect the countries' cyber infrastructure and netizens. The research includes an analysis of the current cybersecurity environment in South Africa. These results were used to develop proposed implementation strategies, structures and sustainment measures, as well as a cybersecurity environment model which can be used for a holistic cybersecurity implementation process that contributes to national security. The study also examines the factors that need to be taken into consideration for the implementation of cybersecurity in Africa.

A new methodology, Morphological Design Engineering (MODE) has been conceptualised and designed and is ideal for the development and implementation of the framework. This mixed-

methods research methodology combines Design Science research methodology, General Morphological Analysis and Ontology Engineering.

The researcher proposes the introduction of a national cybersecurity implementation framework for South Africa to control and protect its cyber infrastructure and netizens, efficiently. This framework contains the proposed implementation strategies and structures that need to be in place, the sustainment measures, as well as a model for the cybersecurity environment that can be used in the implementation process so that national cybersecurity is regarded as an integral part of national security.

South Africa is one of the entry points for broadband into Africa and with the increase in broadband access, any average citizen could become a launch pad for cyberattacks on the rest of the world. This poses a national security threat not only to South Africa but also to the rest of the world. The researcher has put forward a formula to demonstrate the importance of cybersecurity in relation to national security.

In addition to identifying the factors that need to be taken into account to implement cybersecurity in Africa, developing a new methodology for developing and implementing the framework, the researcher also developed a formula to express the importance of cybersecurity towards national security and a cybersecurity policy implementation framework for use in Africa.